

HOW TO OBTAIN LATTICES FROM (f, σ, δ) -CODES VIA A GENERALIZATION OF CONSTRUCTION A

S. PUMPLÜN

ABSTRACT. We show how cyclic (f, σ, δ) -codes over finite rings canonically induce a \mathbb{Z} -lattice in \mathbb{R}^N . The construction can be viewed as a generalization of the classical Construction A for lattices from linear codes and has applications to coset coding, in particular to wire-tap coding. Previous results for lattices obtained from σ -constacyclic codes by Ducoat and Oggier are obtained as special cases.

INTRODUCTION

Recently several classes of linear codes with a better minimal distance for certain lengths than previously known were constructed employing skew polynomial rings $S[t; \sigma, \delta]$ where S is a unital ring, σ an injective endomorphism of S and δ a left σ -derivation of S (e.g. module σ -codes, skew-constacyclic codes etc., see [3], [4], [5], [6], [7], [9], [8] [11], [15], [16], [19], [37]). All these codes are cyclic (f, σ, δ) -codes and built from $S[t; \sigma, \delta]$ by choosing a reducible monic polynomial $f \in S[t; \sigma, \delta]$ of degree m , and some monic right divisor g of f [10].

Rephrasing the theory using nonassociative rings, whenever f is monic, every cyclic (f, σ, δ) -code is associated with a principal left ideal of a unital nonassociative algebra defined by f , which is generated by some monic right divisor g of f : a cyclic (f, σ, δ) -code $\mathcal{C} \subset S^m$ corresponds to a left principal ideal generated by g in an algebra we call S_f and is a free left S -module of dimension $m - \deg g$. The matrix generating such a cyclic (f, σ, δ) -code $\mathcal{C} \subset S^m$ represents the right multiplication R_g in S_f and is a control matrix of \mathcal{C} [29], [30].

The nonassociative algebra $S_f = S[t; \sigma, \delta]/S[t; \sigma, \delta]f$ is defined on the additive subgroup $\{h \in S[t; \sigma, \delta] \mid \deg(h) < m\}$ of $S[t; \sigma, \delta]$ by using right division by f to define the algebra multiplication $g \circ h = gh \bmod_r f$ [30]. We call S_f a *Petit algebra*. Its construction canonically generalizes the one of the associative quotient algebra $S[t; \sigma, \delta]/(f)$, where we factor out a two-sided ideal generated by f , i.e. where f is two-sided (also called invariant). This has several advantages: despite S_f being a nonassociative algebra, its behaviour often is very similar to the associative quotient

Date: 13.7.2016.

2010 Mathematics Subject Classification. Primary: 17A35; Secondary: 11T71, 94B40, 94B05.

Key words and phrases. Space-time block code, linear (f, σ, δ) -code, nonassociative algebra, coset coding, wiretap coding, construction A, order, skew polynomial ring.

algebra $S[t; \sigma, \delta]/(f)$ and our ‘associative intuition’ gained from classical central simple algebras constructed as a quotient $S[t; \sigma, \delta]/(f)$ often makes it easy to work with S_f . We recall that the quotient algebras $S[t; \sigma, \delta]/(f)$ when S is a division algebra, as well as the right nuclei of the algebras S_f were successfully used when constructing central simple algebras for instance in [1], [2], [17], [18, Sections 1.5, 1.8, 1.9], [23].

In this paper we choose suitable monic irreducible skew polynomials f , where either $f \in K[t, \sigma, \delta]$ with K/F a finite field extension of number fields, or $f \in D[t, \sigma, \delta]$ with D a cyclic algebra over a number field, and define natural orders Λ in the division algebra S_f . We investigate the quotient of Λ by certain two-sided ideals of Λ , which is again a Petit algebra. We then use these quotients to canonically construct a lattice L in \mathbb{R}^N , i.e. a \mathbb{Z} -module L of rank N , from a cyclic (f, σ, δ) -code over a finite ring.

The idea behind our construction can be viewed as a generalization of the classical construction A for lattices from linear codes and the setup treated in [14], or also [21], is obtained as the special case where K/F is a cyclic field extension of degree n and the polynomials f used are of the form $f(t) = t^n - c \in \mathcal{O}_F[t; \sigma]$ and two-sided.

[14, Section 5.2, 5.3] hold analogously in our setup and explain how to use our construction for coset coding, i.e. in space-time block coding, in particular for wiretap coding. An additional advantage of using nonassociative algebras for coset coding is the fact that there are several easy conditions available for them to be division. The algebras S_f were already successfully employed to systematically build fast-decodable fully diverse space-time block codes in [26], [33], [20], see [27].

This construction can also be used to assign a (nonassociative) multiplication to lattice codes over number fields, similarly as discussed in [22] in the associative setting. Moreover, classification results on quotients of natural orders as obtained in [21] in the associative setting, can be canonically generalized as well and lead to another new class of nonassociative rings which can be used for coset coding.

The paper is organized as follows: After collecting both the terminology and the results we need in Section 1, we define natural orders in a Petit algebra algebra S_f , $f \in K[t; \sigma, \delta]$ with f monic and irreducible. We investigate the quotients of a natural order by some ideals in Section 2 and show that these quotients again are Petit algebras. This result is then generalized to natural orders in S_f and their quotients by some ideals when $f \in D[t; \sigma, \delta]$ is a monic irreducible skew polynomial, and $D = (K/F, \rho, c)$ a cyclic division algebra, in Section 4. It can thus be applied to a family of algebras employed successfully when designing fast-decodable space-time block codes. In Sections 3 and 5, we describe a lattice encoding of certain cyclic (f, σ, δ) -codes over the finite rings $\mathcal{O}_K/\mathfrak{p}\mathcal{O}_K$, where \mathfrak{p} is a prime ideal in some suitable subring of \mathcal{O}_K , and how it can be applied to space-time block codes.

Throughout the paper we will put a special emphasis on the nonassociative cyclic algebras $(K/F, \sigma, c)$ employed in [34], and on the generalized nonassociative cyclic algebras (D, σ, d) , since these are used for iterated space-time block codes [26], [27]. Dual codes and their lattices are briefly treated in Section 6.

1. PRELIMINARIES

1.1. Nonassociative algebras. Let R be a unital commutative ring and let A be an R -module. We call A an *algebra* over R if there exists an R -bilinear map $A \times A \rightarrow A$, $(x, y) \mapsto x \cdot y$, denoted simply by juxtaposition xy , the *multiplication* of A . An algebra A is called *unital* if there is an element in A , denoted by 1 , such that $1x = x1 = x$ for all $x \in A$. We will only consider unital algebras.

For an R -algebra A , associativity in A is measured by the *associator* $[x, y, z] = (xy)z - x(yz)$. The *left nucleus* of A is defined as $\text{Nuc}_l(A) = \{x \in A \mid [x, A, A] = 0\}$, the *middle nucleus* as $\text{Nuc}_m(A) = \{x \in A \mid [A, x, A] = 0\}$ and the *right nucleus* as $\text{Nuc}_r(A) = \{x \in A \mid [A, A, x] = 0\}$. Their intersection $\text{Nuc}(A) = \{x \in A \mid [x, A, A] = [A, x, A] = [A, A, x] = 0\}$ is the *nucleus* of A . $\text{Nuc}_l(A)$, $\text{Nuc}_m(A)$ and $\text{Nuc}_r(A)$ are associative subalgebras of A containing $R1$ and $x(yz) = (xy)z$ whenever one of the elements x, y, z is in $\text{Nuc}(A)$. The *commuter* of A is defined as $\text{Comm}(A) = \{x \in A \mid xy = yx \text{ for all } y \in A\}$ and the *center* of A is $\text{C}(A) = \{x \in A \mid x \in \text{Nuc}(A) \text{ and } xy = yx \text{ for all } y \in A\}$ [32].

Let R be a Noetherian integral domain with quotient field F and A a finite-dimensional unital F -algebra. Then an R -lattice in A is a finitely generated submodule Γ of A which contains an F -basis of A . An R -order in A is a multiplicatively closed R -lattice containing 1_A (the multiplication may be not associative). An R -order will be called *maximal* if $\Gamma' \subset \Gamma$ implies $\Gamma' = \Gamma$ for every R -order Γ' in A .

An algebra $A \neq 0$ over a field F is called a *division algebra* if for any $a \in A$, $a \neq 0$, the left multiplication with a , $L_a(x) = ax$, and the right multiplication with a , $R_a(x) = xa$, are bijective. Any division algebra is simple, that means has only trivial two-sided ideals. A finite-dimensional algebra A is a division algebra over F if and only if A has no zero divisors.

1.2. Skew polynomial rings. Let S be a unital associative (not necessarily commutative) ring, σ an injective ring homomorphism of S and $\delta : S \rightarrow S$ a *left σ -derivation*, i.e. an additive map such that

$$\delta(ab) = \sigma(a)\delta(b) + \delta(a)b$$

for all $a, b \in S$, implying $\delta(1) = 0$. Let $\text{Const}(\delta) = \{a \in S \mid \delta(a) = 0\}$ and $\text{Fix}(\sigma) = \{a \in S \mid \sigma(a) = a\}$.

The *skew polynomial ring* $R = S[t; \sigma, \delta]$ is the set of skew polynomials

$$a_0 + a_1 t + \cdots + a_n t^n$$

with $a_i \in S$, where addition is defined term-wise and multiplication by

$$ta = \sigma(a)t + \delta(a) \quad (a \in S).$$

We define the *twisted polynomial ring* to be $S[t; \sigma] = S[t; \sigma, 0]$ and the *differential polynomial ring* to be $S[t; \delta] = S[t; id, \delta]$.

For $f = a_0 + a_1t + \cdots + a_nt^n$ with $a_n \neq 0$ define $\deg(f) = n$ and $\deg(0) = -\infty$. Then $\deg(fg) \leq \deg(f) + \deg(g)$ (with equality if h has an invertible leading coefficient, or g has an invertible leading coefficient and σ is injective, or if S is a division ring). An element $f \in R$ is *irreducible* in R if it is no unit and it has no proper factors, i.e if there do not exist $g, h \in R$ with $\deg(g), \deg(h) < \deg(f)$ such that $f = gh$.

1.3. How to obtain nonassociative algebras from skew polynomial rings.

From now on, let $R = S[t; \sigma, \delta]$ and σ injective. We do not assume S to be division. We can still perform a right division by a polynomial $f \in R$ which has invertible leading coefficient d_m : for all $g(t) \in R$ of degree $l > m$, there exist uniquely determined $r(t), q(t) \in R$ with $\deg(r) < \deg(f)$, such that

$$g(t) = q(t)f(t) + r(t).$$

Let $\text{mod}_r f$ denote the remainder of right division by such an f [30, Proposition 1].

Suppose $f(t) = \sum_{i=0}^m d_i t^i \in R = S[t; \sigma, \delta]$ has an invertible leading coefficient d_m . Let $R_m = \{g \in R \mid \deg(g) < m\}$. Then R_m together with the multiplication

$$g \circ h = gh \text{ mod}_r f$$

becomes a unital nonassociative ring $S_f = (R_m, \circ)$ also denoted by R/Rf [30].

This construction was introduced by Petit [24, 25] for unital division rings S . S_f is a unital nonassociative algebra over $S_0 = \{a \in S \mid ah = ha \text{ for all } h \in S_f\}$ which is a commutative subring of S . We call S_f a *Petit algebra*. S_f is associative if and only if Rf is a two-sided ideal in R . For all invertible $a \in S$ we have $S_f \cong S_{af}$, so that without loss of generality it suffices to only consider monic polynomials in the construction.

If S_f is not associative then $S \subset \text{Nuc}_l(S_f)$ and $S \subset \text{Nuc}_m(S_f)$, $\text{Nuc}_r(S_f) = \{g \in R \mid fg \in Rf\}$ and S_0 is the center of S_f [30]. It is easy to see that

$$C(S) \cap \text{Fix}(\sigma) \cap \text{Const}(\delta) \subset S_0.$$

If S is a division algebra and S_f is a finite-dimensional vector space over S_0 , then S_f is a division algebra if and only if $f(t)$ is irreducible in R [24, (9)].

For $f(t) = \sum_{i=0}^m d_i t^i \in S[t; \sigma]$, t is left-invertible if and only if d_0 is invertible by a simple degree argument. Thus if f is irreducible (hence $d_0 \neq 0$) and S a division ring then t is always left-invertible and $S_0 = \text{Fix}(\sigma) \cap C(S)$ is the center of S_f .

Example 1. Let S/S_0 be an extension of commutative unital rings and $G = \langle \sigma \rangle$ a finite cyclic group of order m acting on S such that $S_0 = \text{Fix}(\sigma)$. For any $c \in S$,

$$S_f = S[t; \sigma]/S[t; \sigma](t^m - c)$$

is called the *nonassociative cyclic algebra* $(S/S_0, \sigma, c)$ of degree m . If $c \in S \setminus S_0$, then $(S/S_0, \sigma, c)$ has nucleus S and center S_0 . Over fields, these algebras were studied in [35], they first appeared over finite fields in a paper by Sandler [31]. If $c \in S_0$, this is a cyclic algebra, cf. [14], [21]. Defined over number fields, they were used in code constructions in [34].

Definition 1. Let D be a finite-dimensional central division algebra over $F = \text{Cent}(D)$ of degree n and $\sigma \in \text{Aut}(D)$ such that $\sigma|_F$ has finite order m . A (*generalized*) *nonassociative cyclic algebra of degree m* is an algebra $S_f = D[t; \sigma]/D[t; \sigma]f(t)$ over $F_0 = F \cap \text{Fix}(\sigma)$ with $f(t) = t^m - d \in D[t; \sigma]$. We denote this algebra by (D, σ, d) .

Example 2. Let F and L be fields, $F_0 = F \cap L$, and let K be a cyclic field extension of both F and L such that $\text{Gal}(K/F) = \langle \rho \rangle$ and $[K : F] = n$, $\text{Gal}(K/L) = \langle \sigma \rangle$ and $[K : L] = m$, such that ρ and σ commute. Let $D = (K/F, \rho, c)$ be an associative cyclic division algebra over F of degree n , $c \in F_0$ and $d \in D^\times$. For $x = x_0 + x_1e + x_2e^2 + \cdots + x_{n-1}e^{n-1} \in D$, extend σ to an automorphism $\sigma \in \text{Aut}_L(D)$ of order m via

$$\sigma(x) = \sigma(x_0) + \sigma(x_1)e + \sigma(x_2)e^2 + \cdots + \sigma(x_{n-1})e^{n-1}.$$

For all $d \in D^\times$,

$$S_f = D[t; \sigma]/D[t; \sigma](t^m - d)$$

is the generalized nonassociative cyclic algebra (D, σ, d) of dimension m^2n^2 over F_0 . For all $d \in F^\times$, we have

$$S_f = D[t; \sigma]/D[t; \sigma](t^m - d) = (L/F_0, \gamma, c) \otimes_{F_0} (F/F_0, \sigma, d) = (D, \sigma, d)$$

The algebra is associative iff $d \in F_0$. For $f \in F_0[t]$ the algebra appears in the classical literature on associative central simple algebras as a *generalized cyclic algebra* of degree n in [18, Section 1.4].

The algebras (D, σ, d) with $d \in L^\times$ or $d \in F^\times$ (denoted $It^n(D, \sigma^{-1}, d)$ when $d \in F^\times$ or $It_R^n(D, \sigma^{-1}, d)$ in [27]), are used to construct fast-decodable space-time block codes, the matrix representing their left multiplication yields the codebooks [28], [27], [33]. More precisely, for $m = 2$ this algebra is used in the iterated codes constructed in [20]. When $d \in F^\times$ the algebra is identical to the algebras behind the codes in [33], see also [26].

1.4. Cyclic (f, σ, δ) -codes. Let $f \in S[t; \sigma, \delta]$ be monic of degree m and σ injective. We associate to an element $a(t) = \sum_{i=0}^{m-1} a_i t^i$ in S_f the vector (a_0, \dots, a_{m-1}) . A *linear code of length m over S* is a submodule of the S -module S^m . Conversely, for any linear code \mathcal{C} of length m we denote by $\mathcal{C}(t)$ the set of skew polynomials $a(t) = \sum_{i=0}^{m-1} a_i t^i \in S_f$ associated to the codewords $(a_0, \dots, a_m) \in \mathcal{C}$.

A *cyclic (f, σ, δ) -code* $\mathcal{C} \subset S^m$ is a set consisting of the vectors (a_0, \dots, a_{m-1}) obtained from elements $h = \sum_{i=0}^{m-1} a_i t^i$ in a left principal ideal gS_f where $S_f = S[t; \sigma, \delta]g/S[t; \sigma, \delta]f$, and g is a monic right divisor of f . A code \mathcal{C} over S is called *σ -constacyclic* if there is a non-zero $c \in S$ such that

$$(a_0, \dots, a_{m-1}) \in \mathcal{C} \Rightarrow (\sigma(a_{m-1})c, \sigma(a_0), \dots, \sigma(a_{m-2})) \in \mathcal{C}.$$

Lemma 3. (cf. [30, Proposition 8], [29, Proposition 2])

- (a) Let $f \in R = S[t; \sigma, \delta]$ be monic of degree m and σ be injective. Then:
 - (i) Every right divisor g of f of degree $< m$ has an invertible leading coefficient and generates a principal left ideal in S_f . All left ideals in S_f which contain a non-zero polynomial g of minimal degree with invertible leading coefficient are principal left ideals, and g is a right divisor of f in R .
 - (ii) Each principal left ideal generated by a right divisor of f is an S -module which is isomorphic to a submodule of S^m and forms a code of length m and dimension $m - \deg(g)$.
- (b) Let S be a division ring and $f \in R = S[t; \sigma, \delta]$ be monic of degree m . Then all left ideals in S_f are generated by some monic right divisor g of f in R .

[10, Theorem 2] or the generalization of the proof of [14, Proposition 1] show when h is a parity check polynomial for \mathcal{C} :

Theorem 4. Let $f \in S[t; \sigma, \delta]$ be a monic polynomial and $h = \sum_{i=0}^r h_i t^i \in S[t; \sigma, \delta]$ be a monic polynomial in the center of $S[t; \sigma, \delta]$ such that $f = gh$. Then $f = gh$. Let \mathcal{C} be the cyclic (f, σ, δ) -code corresponding to g and $c \in S^m$, $c(t) = \sum_{i=0}^{m-1} c_i t^i$ the corresponding polynomial. Then the following are equivalent:

- (i) $(c_0, \dots, c_{m-1}) \in \mathcal{C}$.
- (ii) $c(t)h(t) = 0$ in S_f .

The codes \mathcal{C} of length m we consider consist of all elements (a_0, \dots, a_{m-1}) obtained from polynomials $a(t) = \sum_{i=0}^{m-1} a_i t^i$ in a left principal ideal gS_f of S_f , with g a monic right divisor of f . E.g., σ -constacyclic codes are obtained by considering principal left ideals in S_f with $f(t) = t^m - c \in S[t; \sigma]$.

We know that when K is a field, every skew polynomial ring $K[t; \sigma, \delta]$ can be made into either a twisted or a differential polynomial ring by a linear change of variables. When constructing linear codes, however, it helps to consider general skew polynomial rings because these might produce better distance bounds than cyclic (f, σ, δ) -codes constructed only with an automorphism, where $\delta = 0$, e.g. see [6].

2. NATURAL ORDERS IN S_f AND THEIR QUOTIENTS BY A PRIME IDEAL, I

In the following, we use the notation from Section 1.3 and [14, Section 2]. Let K/F be a Galois extension of number fields of degree n . Let \mathcal{O}_F and \mathcal{O}_K be the rings of integers of F and K . We will consider the following setup:

2.1. Let \mathfrak{p} be a prime ideal of \mathcal{O}_F , p the prime lying below \mathfrak{p} and $\mathcal{O}_F/\mathfrak{p}\mathcal{O}_F = \mathbb{F}_{p^j}$, where j is the inertial degree of \mathfrak{p} above p . Let $\pi : \mathcal{O}_K \rightarrow \mathcal{O}_K/\mathfrak{p}\mathcal{O}_K$ be the canonical projection. Let $\sigma \in \text{Gal}(K/F)$. We have $\sigma(\mathfrak{p}\mathcal{O}_K) \subset \mathfrak{p}\mathcal{O}_K$ since $\sigma|_F = \text{id}$. Thus σ induces a ring homomorphism

$$\bar{\sigma} : \mathcal{O}_K/\mathfrak{p}\mathcal{O}_K \rightarrow \mathcal{O}_K/\mathfrak{p}\mathcal{O}_K$$

with $\sigma = \bar{\sigma} \circ \pi$ and $\text{Fix}(\bar{\sigma}) = \mathbb{F}_{p^j}$.

Suppose that δ is an F -linear left σ -derivation on K such that $\delta(\mathcal{O}_K) \subset \mathcal{O}_K$. Then δ induces a left $\bar{\sigma}$ -derivation

$$\bar{\delta} : \mathcal{O}_K/\mathfrak{p}\mathcal{O}_K \rightarrow \mathcal{O}_K/\mathfrak{p}\mathcal{O}_K.$$

We have

$$\mathfrak{p}\mathcal{O}_K = \mathfrak{p}_1^{e_1} \mathfrak{p}_2^{e_2} \cdots \mathfrak{p}_g^{e_g}$$

for suitable prime ideals \mathfrak{p}_i of \mathcal{O}_K , $e_i \geq 0$, since \mathcal{O}_K is a Dedekind domain.

By the Chinese Remainder Theorem, we have the following direct sum of rings:

$$\mathcal{O}_K/\mathfrak{p}\mathcal{O}_K = \mathcal{O}_K/\mathfrak{p}_1^{s_1} \cdots \mathfrak{p}_g^{s_g} \mathcal{O}_K \cong \mathcal{O}_K/\mathfrak{p}_1^{s_1} \mathcal{O}_K \times \cdots \times \mathcal{O}_K/\mathfrak{p}_g^{s_g} \mathcal{O}_K.$$

Moreover, on each ring $\mathcal{O}_K/\mathfrak{p}_1^{s_1}$ there is a canonical induced automorphism $\bar{\sigma}$ and a canonical left $\bar{\sigma}$ -derivation induced by δ .

In particular, if \mathfrak{p} is inert in K/F , $\mathfrak{p}\mathcal{O}_K$ is a prime ideal in \mathcal{O}_K and thus $\mathcal{O}_K/\mathfrak{p}\mathcal{O}_K = \mathbb{F}_{p^{nj}}$ a finite field, and $\bar{\sigma} \in \text{Gal}(\mathbb{F}_{p^{nj}}/\mathbb{F}_{p^j})$ (cf. [14, Section 2] if $\delta = 0$ and K/F is cyclic).

2.2. Suppose

$$f(t) = \sum_{i=0}^m d_i t^i \in \mathcal{O}_K[t; \sigma, \delta]$$

is monic and irreducible in $K[t; \sigma, \delta]$. Consider the division algebra

$$S_f = K[t; \sigma, \delta]/K[t; \sigma, \delta]f$$

over S_0 . Since we keep assuming that $\sigma \in \text{Gal}(K/F)$ and δ is F -linear, here $S_0 = F$. Then the nonassociative \mathcal{O}_F -algebra

$$\Lambda = \mathcal{O}_K[t; \sigma, \delta]/\mathcal{O}_K[t; \sigma, \delta]f$$

is an \mathcal{O}_F -order in S_f called the *natural order*. Note that this order is usually not maximal, but that it is uniquely determined whenever f is not two-sided, since K

is the left and middle nucleus of S_f in that case and uniquely determines \mathcal{O}_K and in turn Λ then.

S_f is associative if and only if f is two-sided. Therefore this definition of a natural order generalizes the natural orders considered in [14] which were only defined for two-sided f and $\delta = 0$. We have

$$\Lambda = \mathcal{O}_K \oplus \mathcal{O}_K t \oplus \cdots \oplus \mathcal{O}_K t^{m-1}$$

as left \mathcal{O}_K -module and

$$\Lambda \otimes_{S_0} K \cong K[t; \sigma, \delta] / K[t; \sigma, \delta]f = S_f.$$

Since f is irreducible in $K[t; \sigma, \delta]$, Λ does not have any zero divisors. The center of Λ contains \mathcal{O}_F . Now since \mathcal{O}_F lies in the center of Λ , for every prime ideal \mathfrak{p} in \mathcal{O}_F , $\mathfrak{p}\Lambda$ is a two-sided ideal of Λ . We have

$$\mathfrak{p}\Lambda = \{al \mid a \in \mathfrak{p}, l \in \Lambda\} = \left\{ \sum_{i=0}^{m-1} a_i t^i \mid a_i \in \mathfrak{p}\mathcal{O}_K \right\}.$$

The surjective homomorphism of nonassociative rings

$$\begin{aligned} \Psi : \Lambda &\longrightarrow (\mathcal{O}_K / \mathfrak{p}\mathcal{O}_K)[t; \bar{\sigma}, \bar{\delta}] / (\mathcal{O}_K / \mathfrak{p}\mathcal{O}_K)[t; \bar{\sigma}, \bar{\delta}]\bar{f} \\ g &\mapsto \bar{g} \end{aligned}$$

has kernel $\mathfrak{p}\Lambda$.

Therefore Ψ induces an isomorphism between the two unital nonassociative rings given by

$$\begin{aligned} \Lambda / \mathfrak{p}\Lambda &\longrightarrow (\mathcal{O}_K / \mathfrak{p}\mathcal{O}_K)[t; \bar{\sigma}, \bar{\delta}] / (\mathcal{O}_K / \mathfrak{p}\mathcal{O}_K)[t; \bar{\sigma}, \bar{\delta}]\bar{f} = S_{\bar{f}} \\ g + \mathfrak{p}\Lambda &\mapsto \bar{g}. \end{aligned}$$

These are unital nonassociative algebras over $\mathcal{O}_F / \mathfrak{p} = \mathbb{F}_{p^j}$. Furthermore, $S_{\bar{f}}$ is associative if and only if $R\bar{f}$ is a two-sided ideal in $R = (\mathcal{O}_K / \mathfrak{p}\mathcal{O}_K)[t; \bar{\sigma}]$. Therefore this generalizes the orders in [14] which appear for two-sided f . In the next example, we point out some differences to the associative case:

Example 5. Let K/F be a Galois extension of degree m , $\text{Gal}(K/F) = \langle \sigma \rangle$ and $A = S_f$ with $f(t) = t^m - c \in \mathcal{O}_K[t; \sigma]$ a twisted polynomial which is irreducible in $K[t; \sigma]$. Then $A = (K/F, \sigma, c)$ is a nonassociative cyclic division algebra of degree m over F . A natural order of A is $\Lambda = \mathcal{O}_K[t; \sigma] / \mathcal{O}_K[t; \sigma]f$, and

$$\Lambda = \mathcal{O}_K \oplus \mathcal{O}_K t \oplus \cdots \oplus \mathcal{O}_K t^{m-1}$$

as a left \mathcal{O}_K -module. The set $\{1, t, t^2, \dots, t^{m-1}\}$ is called the *standard basis* for A .

If $c \in \mathcal{O}_K \setminus \mathcal{O}_F$, A is not associative and Λ is uniquely determined. Put $\bar{c} = c + \mathfrak{p}$ and $\sigma(a + \mathfrak{p}\mathcal{O}_K) = \sigma(a) + \mathfrak{p}\mathcal{O}_K$ for all $a \in \mathcal{O}_K$, then

$$\Lambda / \mathfrak{p}\Lambda \cong ((\mathcal{O}_K / \mathfrak{p}\mathcal{O}_K) / \mathbb{F}_{p^f}, \bar{\sigma}, \bar{c}) = S_{\bar{f}}$$

is an isomorphism between \mathbb{F}_{p^f} -algebras with

$$\overline{f}(t) = t^m - \bar{c} \in (\mathcal{O}_K/\mathfrak{p}\mathcal{O}_K)[t; \overline{\sigma}].$$

If $c \in \mathcal{O}_F$ is non-zero, A is an associative cyclic division algebra, where Λ depends on the choice of the maximal subfield K in A . Then S_f is a cyclic division algebra and

$$S_{\overline{f}} = ((\mathcal{O}_K/\mathfrak{p}\mathcal{O}_K)/(\mathcal{O}_F/\mathfrak{p}\mathcal{O}_F), \overline{\sigma}, \bar{c})$$

is an associative generalized cyclic algebra. This case is covered in [14] and [21].

Remark 6. If $\mathcal{O}_K/\mathfrak{p}\mathcal{O}_K$ is a field and \overline{f} is irreducible in $(\mathcal{O}_K/\mathfrak{p}\mathcal{O}_K)[t; \overline{\sigma}]$ then $S_{\overline{f}}$ is a division algebra. Conversely, if $S_{\overline{f}}$ is a division algebra then $\mathcal{O}_K/\mathfrak{p}\mathcal{O}_K$ must be a field (or else there exist zero divisors in $S_{\overline{f}}$) and so \overline{f} must be irreducible by [24, (9)].

Let Ψ be the above isomorphism of unital nonassociative algebras

$$\Lambda/\mathfrak{p}\Lambda \longrightarrow (\mathcal{O}_K/\mathfrak{p}\mathcal{O}_K)[t; \overline{\sigma}]/(\mathcal{O}_K/\mathfrak{p}\mathcal{O}_K)[t; \overline{\sigma}]\overline{f} = S_{\overline{f}}, \quad g + \mathfrak{p}\Lambda \mapsto \overline{g}.$$

Let \mathcal{I} be a left ideal of Λ such that $\mathfrak{p} \subset \mathcal{I} \cap \mathcal{O}_F$. Then $\mathcal{I}/\mathfrak{p}\Lambda$ is a left ideal of $\Lambda/\mathfrak{p}\Lambda$ and $\Psi(\mathcal{I}/\mathfrak{p}\Lambda)$ is a left ideal of $((\mathcal{O}_K/\mathfrak{p}\mathcal{O}_K), \overline{\sigma}, \bar{c})$.

Remark 7. Suppose that K/F is cyclic and inertial with respect to \mathfrak{p} , then $\mathcal{O}_K/\mathfrak{p}\mathcal{O}_K = \mathbb{F}_{p^{fn}}$ and $\text{Gal}(\mathbb{F}_{p^{fn}}/\mathbb{F}_{p^j}) = \langle \overline{\sigma} \rangle$.

(i) In [14], only the two-sided polynomials $f(t) = t^n - \bar{c}$ with $c \in \mathcal{O}_F$, $\bar{c} = c + \mathfrak{p}$, are considered which makes the ideal in $(\mathcal{O}_K/\mathfrak{p}\mathcal{O}_K)[t; \overline{\sigma}]$ generated by \overline{f} two-sided and the resulting \mathbb{F}_{p^f} -algebra associative. In this case, $\overline{f}(t) = t^n - \bar{c}$ is always reducible in $\mathbb{F}_{p^{fn}}[t; \overline{\sigma}]$.

(ii) By Lemma 3, if \overline{f} is irreducible and $\mathcal{O}_K/\mathfrak{p}\mathcal{O}_K$ a field, then $S_{\overline{f}}$ has no non-trivial left ideals. For instance, if m is a prime and $c \notin \mathcal{O}_F$ (i.e., the algebra is nonassociative) then

$$\Lambda/\mathfrak{p}\Lambda \cong (\mathbb{F}_{p^{jm}}/\mathbb{F}_{p^j}, \overline{\sigma}, \bar{c})$$

is always a semifield, hence $f(t) = t^m - \bar{c}$ irreducible, and so there are no non-trivial left ideals by [29, Proposition 2].

3. LATTICE ENCODING OF CYCLIC (f, σ, δ) -CODES OVER $\mathcal{O}_K/\mathfrak{p}\mathcal{O}_K$, I

3.1. A generalization of Construction A. Let us make the same assumptions on $K[t; \sigma, \delta]$ and f as in Section 2.2. Let $f \in \mathcal{O}_K[t; \sigma, \delta]$ be an irreducible monic skew polynomial, $A = S_f$ and so

$$S_{\overline{f}} = (\mathcal{O}_K/\mathfrak{p}\mathcal{O}_K)[t; \overline{\sigma}, \overline{\delta}]/(\mathcal{O}_K/\mathfrak{p}\mathcal{O}_K)[t; \overline{\sigma}, \overline{\delta}]\overline{f}$$

and

$$\Psi : \Lambda/\mathfrak{p}\Lambda \longrightarrow S_{\overline{f}}, \quad g + \mathfrak{p}\Lambda \mapsto \overline{g}.$$

Let \mathcal{I} be a principal left ideal of Λ such that $\mathfrak{p} \subset \mathcal{I} \cap \mathcal{O}_F$. Then $\mathcal{I}/\mathfrak{p}\Lambda$ is a principal left ideal of $\Lambda/\mathfrak{p}\Lambda$ and $\Psi(\mathcal{I}/\mathfrak{p}\Lambda)$ is a principal left ideal of $((\mathcal{O}_K/\mathfrak{p}\mathcal{O}_K), \bar{\sigma}, \bar{c})$. That means, $\Psi(\mathcal{I}/\mathfrak{p}\Lambda)$ corresponds to an $(\bar{f}, \bar{\sigma}, \bar{c})$ -code \mathcal{C} over \mathbb{F}_q . In particular, if we choose $f(t) = t^m - c$ then $\Psi(\mathcal{I}/\mathfrak{p}\Lambda)$ is a $\bar{\sigma}$ -constacyclic code over \mathbb{F}_q .

Remark 8. If \bar{f} is irreducible and $\mathcal{O}_K/\mathfrak{p}\mathcal{O}_K$ a field, then $S_{\bar{f}}$ has no nontrivial left ideals and so \mathcal{C} has length m and dimension m , or is zero, whereas when \bar{f} is reducible and $\mathcal{O}_K/\mathfrak{p}\mathcal{O}_K$ a field, \mathcal{C} corresponds to a right divisor \bar{g} of \bar{f} and has dimension $m - \deg(\bar{g})$. So we will look for irreducible f where \bar{f} is reducible.

Let

$$\rho : \Lambda \longrightarrow \Lambda/\mathfrak{p}\Lambda \longrightarrow \Psi(\Lambda/\mathfrak{p}\Lambda)$$

be the canonical projection $\Lambda \longrightarrow \Lambda/\mathfrak{p}\Lambda$ composed with Ψ . We know that \mathcal{O}_K is a free \mathbb{Z} -module of rank $n[F : \mathbb{Q}]$. Then

$$L = \rho^{-1}(\mathcal{C}) = \mathcal{I}$$

is a \mathbb{Z} -module of dimension $N = nm[F : \mathbb{Q}]$. The embedding of this lattice into \mathbb{R}^N is canonically determined by considering $A \otimes_{\mathbb{Q}} \mathbb{R}$. Now all works exactly as explained in [14, Section 3.3] (since associativity is not relevant for the argument). The construction of L can again be seen as a (nonassociative) variation of Construction A in [12].

This way we can construct a lattice L in \mathbb{R}^N from the linear code \mathcal{C} over the finite ring $\mathcal{O}_K/\mathfrak{p}\mathcal{O}_K$. The variation of Construction A in [14] is the special case that $f(t) = t^m - a \in \mathcal{O}_F[t] \subset K[t; \sigma]$, where S_f is associative.

3.2. Examples of nonassociative quaternion algebras. Let $K = \mathbb{Q}(i)$, $F = \mathbb{Q}$, so that $\mathcal{O}_F = \mathbb{Z}$ and $\mathcal{O}_K = \mathbb{Z}[i]$. The examples given in [14] are special cases of our construction, using associative generalized cyclic algebras. We now consider some algebras which are not associative:

For any choice of $c \in \mathcal{O}_K \setminus \mathcal{O}_F$, $f(t) = t^2 - c \in \mathcal{O}_K[t, \sigma]$ is irreducible and therefore

$$A = S_f = (\mathbb{Q}(i)/\mathbb{Q}, \sigma, c)$$

a nonassociative quaternion division algebra. We can also write A as the Cayley-Dickson doubling $\text{Cay}(\mathbb{Q}(i), c)$, defined in the obvious way. For the natural order

$$\Lambda = \mathbb{Z}[i] \oplus \mathbb{Z}[i]e$$

and any prime ideal \mathfrak{p} in \mathcal{O}_F , we get the nonassociative generalized quaternion algebra

$$\Lambda/\mathfrak{p}\Lambda \cong ((\mathcal{O}_K/\mathfrak{p}\mathcal{O}_K)/\mathbb{F}_{p^2}, \bar{\sigma}, \bar{c}) = S_{\bar{f}}$$

with

$$\bar{f}(t) = t^2 - \bar{c} \in (\mathcal{O}_K/\mathfrak{p}\mathcal{O}_K)[t; \bar{\sigma}].$$

In particular, we have

$$\Lambda/\mathfrak{p}\Lambda = (\mathcal{O}_K/\mathfrak{p}\mathcal{O}_K) \oplus (\mathcal{O}_K/\mathfrak{p}\mathcal{O}_K)e$$

as $(\mathcal{O}_K/\mathfrak{p}\mathcal{O}_K)$ -module.

Example 9. Choose any p which remains inert in $\mathbb{Q}(i)$, then $\mathcal{O}_K/\mathfrak{p}\mathcal{O}_K = \mathbb{F}_{p^{2j}}$, where j is the inertial degree of \mathfrak{p} above p , and

$$\Lambda/\mathfrak{p}\Lambda \cong (\mathbb{F}_{p^{2j}}/\mathbb{F}_{p^j}, \bar{\sigma}, \bar{c})$$

is a semifield because $f(t) = t^2 - \bar{c}$ is irreducible. Therefore primes p which remain inert in $\mathbb{Q}(i)$ do not yield algebras which are suitable for lattice encoding, as there are no nontrivial left ideals in $(\mathbb{F}_{p^{2j}}/\mathbb{F}_{p^j}, \bar{\sigma}, \bar{c})$. Thus given any left ideal \mathcal{I} of Λ containing \mathfrak{p} , $\Psi(\mathcal{I}/\mathfrak{p}\Lambda)$ is either trivial or all of $S_{\bar{\mathcal{f}}} = \mathbb{F}_{p^{2j}}[t; \bar{\sigma}]/(\mathbb{F}_{p^{2j}}[t; \bar{\sigma}])\bar{f}$.

E.g., take $p = 3$ and $c = i$. Then

$$\Lambda/3\Lambda \cong (\mathbb{F}_9/\mathbb{F}_3, \bar{\sigma}, \bar{i})$$

is a division algebra over \mathbb{F}_3 where $\bar{\sigma}(\alpha) = \alpha^3$, if α is a primitive root of \mathbb{F}_9 over \mathbb{F}_3 , that is $\alpha^2 + 1 = 0$. $\mathcal{I} = (1 + i)\Lambda$ satisfies $3 \in \mathcal{I} \cap \mathcal{O}_F$ (since $1 - 2i \in \mathbb{Z}[i]$, so $(1 + i)(1 - 2i) = 3 \in \mathcal{I}$). Hence $\mathcal{I}/3\Lambda$ is a left principal ideal of $\Lambda/3\Lambda \cong (\mathbb{F}_9/\mathbb{F}_3, \bar{\sigma}, \bar{i})$, generated by $\Psi((1 + i) + 3\Lambda)$, implying $\mathcal{I}/3\Lambda \cong (\mathbb{F}_9/\mathbb{F}_3, \bar{\sigma}, \bar{i})$.

Example 10. Choose any p which splits in $\mathbb{Q}(i)$, e.g. $p = 5$. Then $(5) = (1 + 2i)(1 - 2i)$ means that

$$\mathbb{Z}[i]/5\mathbb{Z}[i] \cong \mathbb{Z}[i]/(1 - 2i) \times \mathbb{Z}[i]/(1 + 2i) \cong \mathbb{F}_5 \times \mathbb{F}_5$$

and

$$\Lambda/5\Lambda = (\mathbb{F}_5 \times \mathbb{F}_5) \oplus (\mathbb{F}_5 \times \mathbb{F}_5)e$$

is a generalized nonassociative quaternion algebra over \mathbb{F}_5 and we have the following algebra isomorphism:

$$\Lambda/5\Lambda \cong ((\mathbb{F}_5 \times \mathbb{F}_5)/\mathbb{F}_5, \bar{\sigma}, \bar{c}) = S_{\bar{\mathcal{f}}}$$

with

$$\bar{\mathcal{f}}(t) = t^2 - \bar{c} \in (\mathbb{F}_5 \times \mathbb{F}_5)[t; \bar{\sigma}].$$

Here, $\bar{\sigma}(a, b) = (b, a)$ fixes the elements (a, a) , $a \in \mathbb{F}_5$. The algebra $\Lambda/5\Lambda$ is a split nonassociative quaternion algebra [36] and thus $\bar{\mathcal{f}}$ is reducible in $(\mathbb{F}_5 \times \mathbb{F}_5)[t; \bar{\sigma}]$. This setup can be used for lattice encoding of $\bar{\sigma}$ -constacyclic codes, which correspond to principal left ideals of $S_{\bar{\mathcal{f}}}$.

Example 11. Choose $p = 2$ which ramifies in $\mathbb{Q}(i)$. Then $\mathbb{Z}[i]/2\mathbb{Z}[i] \cong \mathbb{F}_2 + \mathbb{F}_2v = \{0, 1, v, v + 1\}$ with $v^2 = 0$. I.e., $\mathbb{F}_2 + \mathbb{F}_2v$ is the finite chain ring of characteristic 2, nilpotency index 2 and residue field \mathbb{F}_2 . Here $\bar{\sigma} = id$,

$$\Lambda/2\Lambda = (\mathbb{F}_2 + \mathbb{F}_2v) \oplus (\mathbb{F}_2 + \mathbb{F}_2v)e$$

and we have the following \mathbb{F}_2 -algebra isomorphism:

$$\Lambda/2\Lambda \cong ((\mathbb{F}_2 + \mathbb{F}_2 v)/\mathbb{F}_2, id, \bar{c}) = S_{\bar{f}}$$

with $\bar{f}(t) = t^2 - \bar{c} \in (\mathbb{F}_2 + \mathbb{F}_2 v)[t]$, $c \in \mathcal{O}_K \setminus \mathcal{O}_F$. For both possible \bar{f} , i.e. $\bar{f}(t) = t^2 - \bar{c}$ with $\bar{c} = v$ or $\bar{c} = v + 1$, it is easy to show that \bar{f} is irreducible. We conclude that $p = 2$ does not yield an algebra which can be employed for lattice encoding.

Note that if we choose any p which ramifies in $\mathbb{Q}(i)$ then p induces an algebra useful for lattice encoding of a $\bar{\sigma}$ -constacyclic code, whenever \bar{f} is reducible.

For any p which ramifies in $\mathbb{Q}(i)$, the corresponding algebra contains zero divisors for any choice of f , with \bar{f} reducible or not.

4. NATURAL ORDERS IN S_f AND THEIR QUOTIENTS BY A PRIME IDEAL, II

In the following, we use the notation from Sections 1.3 and 2.

4.1. Let K/F be a cyclic Galois extension of number fields of degree n with $\text{Gal}(K/F) = \langle \rho \rangle$. Let \mathcal{O}_F and \mathcal{O}_K be the corresponding rings of integers. Let $D = (K/F, \rho, c)$ be a cyclic division algebra over F such that $c \in \mathcal{O}_F^\times$. Let $\mathcal{D} = (\mathcal{O}_K/\mathcal{O}_F, \rho, c)$ be the generalized associative cyclic algebra over \mathcal{O}_F of degree n such that $\mathcal{D} \otimes_{\mathcal{O}_F} F = (K/F, \rho, c) = D$. Then

$$\mathcal{D} = \mathcal{O}_K \oplus \mathcal{O}_K e \oplus \cdots \oplus \mathcal{O}_K e^{n-1}$$

is a natural \mathcal{O}_F -order of D , cf. 2.2 or [14].

Let $\sigma \in \text{Aut}(D)$ and δ be a σ -derivation on D , satisfying the following criteria:

- $F_0 = F \cap \text{Fix}(\sigma) \cap \text{Const}(\delta)$ is a number field.
- $\sigma(\mathcal{D}) \subset \mathcal{D}$ and $\delta(\mathcal{D}) \subset \mathcal{D}$.
- $S_0 = \mathcal{O}_F \cap \text{Fix}(\sigma) \cap \text{Const}(\delta)$ is the ring of integers of F_0 where here σ and δ denote the restrictions of σ and δ to \mathcal{D} .

Suppose

$$f(t) = \sum_{i=0}^m d_i t^i \in \mathcal{D}[t; \sigma, \delta]$$

is monic and irreducible in $D[t; \sigma, \delta]$. Consider the division algebra

$$S_f = D[t; \sigma, \delta]/D[t; \sigma, \delta]f$$

over F_0 . Then the S_0 -algebra

$$\Lambda = \mathcal{D}[t; \sigma, \delta]/\mathcal{D}[t; \sigma, \delta]f$$

is an S_0 -order in S_f which we call the *natural order* (this is again usually not maximal). If $1, e, \dots, e^{n-1}$ is the canonical basis of D then we have

$$\Lambda = \mathcal{O}_K \oplus \mathcal{O}_K e \oplus \cdots \oplus \mathcal{O}_K e^{n-1} \oplus \mathcal{O}_K t \oplus \mathcal{O}_K e t \oplus \cdots \oplus \mathcal{O}_K e^{n-1} t \oplus \cdots \oplus \mathcal{O}_K e^{n-1} t^{m-1}$$

as left \mathcal{O}_K -module and

$$\Lambda \otimes_{S_0} F \cong D[t; \sigma]/D[t; \sigma]f = S_f.$$

Since f is irreducible in $D[t; \sigma, \delta]$, Λ does not have zero divisors.

Remark 12. Here, a natural order Λ is not uniquely determined even when f is not two-sided. It still depends on the choice of the maximal subfield in D . We will assume K fixed as above.

The center of Λ contains S_0 . Let \mathfrak{p} be a prime ideal in S_0 . Since S_0 lies in the centers of both \mathcal{D} and of Λ , $\mathfrak{p}\mathcal{D}$ is a two-sided ideal of \mathcal{D} and $\mathfrak{p}\Lambda$ is a two-sided ideal of Λ . Let $\pi : \mathcal{D} \rightarrow \mathcal{D}/\mathfrak{p}\mathcal{D}$ be the canonical projection. We have $\sigma(\mathfrak{p}\mathcal{D}) \subset \mathfrak{p}\mathcal{D}$ since $\mathfrak{p} \subset \text{Fix}(\sigma)$ and $\sigma(\mathcal{D}) \subset \mathcal{D}$ by assumption. Thus σ induces a ring homomorphism

$$\bar{\sigma} : \mathcal{D}/\mathfrak{p}\mathcal{D} \rightarrow \mathcal{D}/\mathfrak{p}\mathcal{D}$$

with

$$\text{Fix}(\bar{\sigma}) = \text{Fix}(\sigma)/\mathfrak{p}\text{Fix}(\sigma)$$

and $\sigma = \bar{\sigma} \circ \pi$. We also have $\delta(\mathfrak{p}\mathcal{D}) \subset \mathfrak{p}\mathcal{D}$ by assumption. That means δ induces a left $\bar{\sigma}$ -derivation

$$\bar{\delta} : \mathcal{D}/\mathfrak{p}\mathcal{D} \rightarrow \mathcal{D}/\mathfrak{p}\mathcal{D}$$

with field of constants

$$\text{Const}(\bar{\delta}) = \text{Const}(\delta)/\mathfrak{p}.$$

The the surjective homomorphism of nonassociative rings

$$\Psi : \Lambda \rightarrow (\mathcal{D}/\mathfrak{p}\mathcal{D})[t; \bar{\sigma}, \bar{\delta}]/(\mathcal{D}/\mathfrak{p}\mathcal{D})[t; \bar{\sigma}, \bar{\delta}]\bar{f}$$

$$g \mapsto \bar{g}$$

has kernel $\mathfrak{p}\Lambda$ and induces an isomorphism of unital nonassociative algebras

$$\Lambda/\mathfrak{p}\Lambda \cong (\mathcal{D}/\mathfrak{p}\mathcal{D})[t; \bar{\sigma}, \bar{\delta}]/(\mathcal{D}/\mathfrak{p}\mathcal{D})[t; \bar{\sigma}, \bar{\delta}]\bar{f}$$

$$g + \mathfrak{p}\Lambda \mapsto \bar{g}$$

over

$$\bar{S}_0 = \text{Fix}(\bar{\sigma}) \cap \text{Const}(\bar{\delta}) \cap \bar{F}$$

with $\bar{F} = \mathcal{O}_F/\mathfrak{p}\mathcal{O}_F = \mathbb{F}_{p^j}$, where j is the inertial degree of \mathfrak{p} above p .

Remark 13. Note that even if $R = D[t; \sigma, \delta]$ is isomorphic to $D[t; \sigma]$ or $D[t; \delta]$, like when σ or δ are inner, the codes we obtain from using different ways to write R can be substantially different in performance.

4.2. Example. Let F , L and K be number fields and let K be a cyclic extension of both F and L such that

- (1) $\text{Gal}(K/F) = \langle \rho \rangle$ and $[K : F] = n$,
- (2) $\text{Gal}(K/L) = \langle \sigma \rangle$ and $[K : L] = m$,
- (3) ρ and σ commute

as in Example 2. Let $F_0 = F \cap L$. Let $\mathcal{D} = (\mathcal{O}_K/\mathcal{O}_F, \rho, c)$, $c \in \mathcal{O}_{F_0}$, be an associative cyclic algebra over \mathcal{O}_F of degree n such that $D = (K/F, \rho, c) = \mathcal{D} \otimes_{\mathcal{O}_F} F$ is a division algebra over F . For $x = x_0 + ex_1 + e^2x_2 + \cdots + e^{n-1}x_{n-1} \in D$, define

$$\sigma(x) = \sigma(x_0) + \sigma(x_1)e + \sigma(x_2)e^2 + \cdots + \sigma(x_{n-1})e^{n-1}.$$

Since $c \in \mathcal{O}_{F_0}$, $\sigma \in \text{Aut}_L(D)$ has order m and restricts to $\sigma \in \text{Aut}_{\mathcal{O}_L}(\mathcal{D})$.

The F_0 -algebra $S_f = (D, \sigma, d)$ where $f(t) = t^m - d \in D[t; \sigma]$ and $d \in \mathcal{O}_L^\times$ or $d \in \mathcal{O}_F^\times$, is a right K -vector space of dimension mn .

Let \mathfrak{p} be a prime ideal in \mathcal{O}_{F_0} . Then there is an algebra isomorphism

$$\Lambda/\mathfrak{p}\Lambda \cong (\mathcal{D}/\mathfrak{p}\mathcal{D})[t; \bar{\sigma}]/(\mathcal{D}/\mathfrak{p}\mathcal{D})[t; \bar{\sigma}]\bar{f}$$

$$g + \mathfrak{p}\Lambda \mapsto \bar{g}.$$

These are algebras over $\overline{F_0} = \mathcal{O}_{F_0}/\mathfrak{p}$ and the quotient $\Lambda/\mathfrak{p}\Lambda$ is isomorphic to the $\overline{F_0}$ -algebra

$$(\overline{D}, \bar{\sigma}, \bar{d}),$$

where

$$\overline{D} = \mathcal{D}/\mathfrak{p}\mathcal{D}$$

is a generalized associative cyclic algebra over $\mathbb{F}_{p^j} = \text{Fix}(\bar{\rho})$.

4.3. Example. Let ω denote the primitive third root of unity and $\theta = \omega_7 + \omega_7^{-1} = 2\cos(\frac{2\pi}{7})$ where ω_7 is a primitive 7th root of unity and put $F = \mathbb{Q}(\theta)$. Let $K = F(\omega) = \mathbb{Q}(\omega, \theta)$ and consider the quaternion division algebra $D = (K/F, \sigma, -1)$. Note that $\sigma : i \mapsto -i$ and therefore $\sigma(\omega) = \omega^2$. Finally, we let $L = \mathbb{Q}(\omega)$ so that K/L is a cubic cyclic field extension whose Galois group is generated by the automorphism $\tau : \zeta_7 + \zeta_7^{-1} \mapsto \zeta_7^2 + \zeta_7^{-2}$. Note that $\omega \in \mathcal{O}_L = \mathbb{Z}[\omega]$. It was shown in [33] that $A = (D, \tau^{-1}, \omega) = It_R^3(D, \tau, \omega)$, the algebra behind the codes employed in [33] (cf. [26]), is a division algebra, so that the codes are fully diverse. Observe that

$$\Lambda = \mathbb{Z}[\omega_3, \omega_7 + \omega_7^{-1}] \oplus \mathbb{Z}[\omega_3, \omega_7 + \omega_7^{-1}]e \oplus \mathbb{Z}[\omega_3, \omega_7 + \omega_7^{-1}]e^2 \oplus \cdots$$

is a natural order in A .

Let $p = 2$, then \mathfrak{p} is a prime ideal in $\mathcal{O}_F = \mathbb{Z}[\omega_3]$ which remains prime in $\mathcal{O}_K = \mathbb{Z}[\omega_3, \omega_7 + \omega_7^{-1}]$ and $\mathbb{Z}[i]/\mathfrak{p} \cong \mathbb{F}_4$. \mathfrak{p} is inert in $K = \mathbb{Q}(\omega_3, \omega_7 + \omega_7^{-1})$. Now

$$\mathcal{D}/\mathfrak{p}\mathcal{D} = (\mathbb{F}_{64}/\mathbb{F}_8, \bar{\sigma}, -1) \cong \text{Mat}_2(\mathbb{F}_8)$$

is a split quaternion algebra over \mathbb{F}_8 . Thus

$$\Lambda/\mathfrak{p}\Lambda \cong (\text{Mat}_2(\mathbb{F}_8), \bar{\tau}^{-1}, \bar{\omega})$$

where $\bar{\omega} \in \mathbb{Z}[\omega]/2\mathbb{Z}[\omega]$.

5. LATTICE ENCODING OF CYCLIC (f, σ, δ) -CODES OVER $\mathcal{O}_K/\mathfrak{p}\mathcal{O}_K$, II

5.1. A second generalization of Construction A. Assume the setup from Section 4.1, i.e. let $\mathcal{D} = (\mathcal{O}_K/\mathcal{O}_F, \rho, c)$ be a generalized associative cyclic algebra over \mathcal{O}_F of degree n such that $D = (K/F, \rho, c) = \mathcal{D} \otimes_{\mathcal{O}_F} F$, $\sigma \in \text{Aut}(D)$, δ be a σ -derivation on D , such that both satisfy the criteria from Section 4.1 and let

$$f(t) = \sum_{i=0}^m d_i t^i \in \mathcal{D}[t; \sigma, \delta]$$

be monic and irreducible in $D[t; \sigma, \delta]$. Consider the division algebra

$$S_f = D[t; \sigma, \delta]/D[t; \sigma, \delta]f$$

over F_0 . For a prime ideal \mathfrak{p} in S_0 and

$$\Lambda = \mathcal{D}[t; \sigma, \delta]/\mathcal{D}[t; \sigma, \delta]f$$

let

$$S_{\bar{f}} = (\mathcal{D}/\mathfrak{p}\mathcal{D})[t; \bar{\sigma}, \bar{\delta}]/(\mathcal{D}/\mathfrak{p}\mathcal{D})[t; \bar{\sigma}, \bar{\delta}]\bar{f}.$$

Then

$$\Psi : \Lambda/\mathfrak{p}\Lambda \cong S_{\bar{f}}, \quad g + \mathfrak{p}\Lambda \mapsto \bar{g}$$

is an isomorphism between algebras as in Section 4.1. Since we know that

$$S_0/\mathfrak{p} \cong \text{Fix}(\bar{\sigma}) \cap \text{Const}(\bar{\delta}) \cap \bar{F}$$

with $\bar{F} = \mathcal{O}_F/\mathfrak{p}\mathcal{O}_F = \mathbb{F}_{p^j}$, where j is the inertial degree of \mathfrak{p} above p , these are algebras over a subfield of \mathbb{F}_{p^j} .

Let \mathcal{I} be a principal left ideal of Λ such that $\mathfrak{p} \subset \mathcal{I} \cap S_0$. Then $\mathcal{I}/\mathfrak{p}\Lambda$ is a non-zero principal left ideal of $\Lambda/\mathfrak{p}\Lambda$ and $\Psi(\mathcal{I}/\mathfrak{p}\Lambda)$ is a principal left ideal of $S_{\bar{f}}$. That means $\Psi(\mathcal{I}/\mathfrak{p}\Lambda)$ corresponds to an $(\bar{f}, \bar{\sigma}, \bar{\delta})$ -code \mathcal{C} over $\mathcal{O}_K/\mathfrak{p}\mathcal{O}_K$.

In particular, if we choose $\delta = 0$ and $f(t) = t^m - c \in \mathcal{D}[t; \sigma]$ then $\Psi(\mathcal{I}/\mathfrak{p}\Lambda)$ is a $\bar{\sigma}$ -constacyclic code over $\mathcal{O}_K/\mathfrak{p}\mathcal{O}_K$.

If \bar{f} is irreducible and $\mathcal{D}/\mathfrak{p}\mathcal{D}$ is a division algebra, then the algebra $S_{\bar{f}}$ is simple. Then any non-zero code \mathcal{C} must have length m and dimension m (and correspond to the whole algebra), whereas whenever \bar{f} is reducible, \mathcal{C} respectively $\Psi(\mathcal{I}/\mathfrak{p}\Lambda)$ corresponds to a right divisor \bar{g} of \bar{f} and has dimension $m - \deg(\bar{g})$. Let

$$\rho : \Lambda \longrightarrow \Lambda/\mathfrak{p}\Lambda \longrightarrow \Psi(\Lambda/\mathfrak{p}\Lambda)$$

be the canonical projection $\Lambda \longrightarrow \Lambda/\mathfrak{p}\Lambda$ composed with Ψ . We know that \mathcal{O}_K is a free \mathbb{Z} -module of rank $n[F : \mathbb{Q}]$. Therefore

$$L = \rho^{-1}(\mathcal{C}) = \mathcal{I}$$

is a \mathbb{Z} -module of dimension $N = n^2 m[F : \mathbb{Q}]$. The embedding of this lattice into \mathbb{R}^N is canonically determined by considering $A \otimes_{\mathbb{Q}} \mathbb{R}$. Again all works exactly as explained in [14, Section 3.3] (since associativity is not relevant for the argument). The construction of L can again be seen as a second (nonassociative) variation of Construction A in [12].

This way we can construct a lattice L in \mathbb{R}^N from the linear $(\bar{f}, \bar{\sigma}, \bar{\delta})$ -code \mathcal{C} over a finite ring.

5.2. Space-time block codes. We can apply the above considerations to space-time block coding as we demonstrate in the next two examples.

Example 14. Let $A = (K/F, \sigma, d)$, $d \in \mathcal{O}_K$ non-zero, be a nonassociative cyclic division algebra of degree m as in Example 5, so that $f(t) = t^m - c \in \mathcal{O}_K[t; \sigma]$ is irreducible in $K[t; \sigma]$. Take the natural order $\Lambda = \mathcal{O}_K[t; \sigma]/\mathcal{O}_K[t; \sigma]f$, and let $a = a_0 + a_1 t + \dots + a_{m-1} t^{m-1}$, $b = b_0 + b_1 t + \dots + b_{m-1} t^{m-1} \in \Lambda$. If we represent the elements of Λ as vectors $a = (a_0, a_1, \dots, a_{m-1})$, $b = (b_0, b_1, \dots, b_{m-1})^T$, then we can write the nonassociative multiplication in Λ as the matrix multiplication $ab = \lambda(a)b$ where $\lambda(a)$ is an $m \times m$ matrix with entries in \mathcal{O}_K :

$$(1) \quad \lambda(a) = \begin{bmatrix} a_0 & c\sigma(a_{m-1}) & c\sigma^2(a_{m-2}) & \dots & c\sigma^{m-1}(a_1) \\ a_1 & \sigma(a_0) & c\sigma^2(a_{m-1}) & \dots & c\sigma^{m-1}(a_2) \\ a_2 & \sigma(a_1) & \sigma^2(a_0) & \dots & c\sigma^{m-1}(a_3) \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_{m-1} & \sigma(a_{m-2}) & \sigma^2(a_{m-3}) & \dots & \sigma^{m-1}(a_0) \end{bmatrix}.$$

Let $\mathfrak{p} \subset \mathcal{O}_F$ be a prime ideal. Then the isomorphism $\Lambda/\mathfrak{p}\Lambda \cong ((\mathcal{O}_K/\mathfrak{p}\mathcal{O}_K)/\mathbb{F}_{p^f}, \bar{\sigma}, \bar{c})$ given by Ψ yields the canonical projection

$$\rho : \Lambda \longrightarrow \Lambda/\mathfrak{p}\Lambda \longrightarrow \Psi(\Lambda/\mathfrak{p}\Lambda).$$

Hence

$$L = \rho^{-1}(\mathcal{C}) = \mathcal{I}$$

is a fully diverse space-time block code over \mathcal{O}_K which is a \mathbb{Z} -lattice whose embedding into \mathbb{R}^m is canonically determined by $A \otimes_{\mathbb{Q}} \mathbb{R}$.

Nonassociative cyclic division algebras as above can be employed to obtain fully diverse multiple-input double-output codes [34]. The algebras $A = (D, \sigma^{-1}, d)$ we consider next are used for the systematic space-time block code constructions of the fast-decodable iterated codes in [28], [27], [33].

Example 15. Let $A = (D, \sigma^{-1}, d)$ be a division algebra of degree n with D, σ etc. defined as in Section 4.2 and $d \in \mathcal{O}_L$ or $d \in \mathcal{O}_F$.

For $x = x_0 + x_1t + x_2t^2 + \cdots + x_{m-1}t^{m-1}$, $y = y_0 + y_1t + y_2t^2 + \cdots + y_{m-1}t^{m-1} \in \Lambda$, $x_i, y_i \in \mathcal{D}$, represent x as $(x_0, x_1, \dots, x_{m-1})$ and y as a column vector $(y_0, y_1, \dots, y_{m-1})^T$, then we can write the product of x and y in Λ as a matrix multiplication $xy = M(x)y$, where $M(x)$ is an $m \times m$ matrix with entries in \mathcal{D} given by

$$M(x) = \begin{bmatrix} x_0 & d\sigma^{-1}(x_{m-1}) & d\sigma^{-2}(x_{m-2}) & \cdots & d\sigma^{-(m-1)}(x_1) \\ x_1 & \sigma^{-1}(x_0) & d\sigma^{-2}(x_{m-1}) & \cdots & d\sigma^{-(m-1)}(x_2) \\ x_2 & \sigma^{-1}(x_1) & \sigma^{-2}(x_0) & \cdots & d\sigma^{-(m-1)}(x_3) \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ x_{m-1} & \sigma^{-1}(x_{m-2}) & \sigma^{-2}(x_{m-3}) & \cdots & \sigma^{-(m-1)}(x_0) \end{bmatrix}$$

Writing elements in $\Lambda = \mathcal{O}_K \oplus \mathcal{O}_K e \oplus \cdots \oplus \mathcal{O}_K e^{n-1}t^{m-1}$ as column vectors of length mn with entries in \mathcal{O}_K , we obtain $xy = \lambda(M(x))y$, where

$$(2) \quad \lambda(M(x)) = \begin{bmatrix} \lambda(x_0) & \lambda(d)\sigma^{-1}(\lambda(x_{m-1})) & \cdots & \lambda(d)\sigma^{-(m-1)}(\lambda(x_1)) \\ \lambda(x_1) & \sigma^{-1}(\lambda(x_0)) & \cdots & \lambda(d)\sigma^{-(m-1)}(\lambda(x_2)) \\ \vdots & \vdots & \ddots & \vdots \\ \lambda(x_{m-1}) & \sigma^{-1}(\lambda(x_{m-2})) & \cdots & \sigma^{-(m-1)}(\lambda(x_0)) \end{bmatrix}$$

is the $mn \times mn$ matrix with entries in \mathcal{O}_K obtained by taking the left regular representation in \mathcal{D} of each entry in the matrix $M(x)$. It represents left multiplication in Λ . This family of matrices induces a fully diverse linear space-time block code, and this construction is used in [33], [20], [27]. In particular, if $d \in \mathcal{O}_F$, then $\det(\lambda(M(x))) \in \mathcal{O}_F$ ([20], [27, Remark 5]). And if $d \in \mathcal{O}_L$, then

$$(3) \quad \lambda(M(x)) = \begin{bmatrix} \lambda(x_0) & d\sigma^{-1}(\lambda(x_{n-1})) & d\sigma^{-2}(\lambda(x_{n-2})) & \cdots & d\sigma^{-(m-1)}(\lambda(x_1)) \\ \lambda(x_1) & \sigma^{-1}(\lambda(x_0)) & d\sigma^{-2}(\lambda(x_{n-1})) & \cdots & d\sigma^{-(m-1)}(\lambda(x_2)) \\ \lambda(x_2) & \sigma^{-1}(\lambda(x_1)) & \sigma^{-2}(\lambda(x_0)) & \cdots & d\sigma^{-(m-1)}(\lambda(x_3)) \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \lambda(x_{n-1}) & \sigma^{-1}(\lambda(x_{n-2})) & \sigma^{-2}(\lambda(x_{n-3})) & \cdots & \sigma^{-(m-1)}(\lambda(x_0)) \end{bmatrix}$$

and $\det(\lambda(M(x))) \in L \cap \mathcal{O}_K = \mathcal{O}_L$ ([33], [27, Lemma 19]).

Let $\mathfrak{p} \subset \mathcal{O}_{F_0}$ be a prime ideal. Then $\Lambda/\mathfrak{p}\Lambda \cong (\overline{D}, \overline{\sigma}, \overline{d})$ via Ψ and this isomorphism yields the canonical projection

$$\rho : \Lambda \longrightarrow \Lambda/\mathfrak{p}\Lambda \longrightarrow \Psi(\Lambda/\mathfrak{p}\Lambda).$$

Here,

$$L = \rho^{-1}(\mathcal{C}) = \mathcal{I}$$

induces a fully diverse space-time block code over \mathcal{O}_K which is a \mathbb{Z} -lattice whose embedding into \mathbb{R}^N , $N = mn^2$, is canonically determined by $A \otimes_{\mathbb{Q}} \mathbb{R}$.

Remark 16. The explanations in [14, Section 5.2, 5.3] hold analogously for our generalization of Construction A in Section 5.1 and the examples here, and show the potential of the construction for coset coding used in space-time block coding, in particular for wiretap space-time block coding, but also for linear codes over finite rings. The fact that in our setting the lattices L were obtained from a nonassociative division algebra is irrelevant. Moreover, the matrix generating a cyclic (f, σ, δ) -code $\mathcal{C} \subset S^m$ represents the right multiplication R_g in S_f and is a control matrix of \mathcal{C} [29], [30].

6. DUAL CODES

We briefly sketch how dual codes relate to our construction, generalizing results from [14, Section 4]. Recall that the dual code of a linear code \mathcal{C} in S^m is defined as

$$\mathcal{C}^\perp = \{b \mid \langle b, c \rangle = 0 \text{ for all } c \in \mathcal{C}\}$$

where \langle, \rangle denotes the Euclidean product in S^m .

For the sake of simplicity, we only consider the situation that $f \in S[t; \sigma]$, where S is a commutative integral domain (i.e. $S = \mathcal{O}_K/\mathfrak{p}\mathcal{O}_K$ in our set-up, the argument below however works for any commutative integral domain S), although all observations can be generalized to the setup that δ is not trivial and D a cyclic algebra. This allows us to apply [14, Proposition 2] without generalizing the statement first. Let

$$\theta : (\mathcal{O}_K/\mathfrak{p}\mathcal{O}_K)[t; \sigma] \longrightarrow (\mathcal{O}_K/\mathfrak{p}\mathcal{O}_K)[t^{-1}; \sigma^{-1}], \quad \sum_{i=0}^m a_i t^i \mapsto \sum_{i=0}^m t^{-i} a_i$$

be the anti-isomorphism of rings from [14, Proposition 2]. Let $S = \mathcal{O}_K/\mathfrak{p}\mathcal{O}_K$, $f \in S[t; \sigma]$ be monic and \mathcal{C} be an (f, σ) -code associated with $g(t)$ with monic parity check polynomial $h(t) = \sum_{i=0}^k h_i t^i$, so that $h(t)g(t) = f(t)$. In order to obtain generalizations of [14, Proposition 2] for any choice of f , where the dual code is an $(f, \sigma, 0)$ -code again, we will make strong restrictions on the polynomials f , h and g involved.

Proposition 17. *Let \mathcal{C} be a $(f, \sigma, 0)$ -code associated with $g(t)$ with monic parity check polynomial $h(t) = \sum_{i=0}^m h_i t^i$, so that $h(t)g(t) = f(t) = g(t)h(t)$. Suppose that*

- (i) $a_0 \in \text{Fix}(\sigma)$ is invertible,*
- (ii) $a_i = a_0^{-1} \sigma^{m-k-i}(a_{m-i})$ for all i , $0 \leq i \leq m$. Define*

$$g^\perp(t) = \sum_{j=0}^k \sigma^{-j}(h_{k-j}) t^j$$

and assume that g^\perp is a right divisor of f . Then the $(f, \sigma, 0)$ -constacyclic code associated with $g^\perp(t)$ is the Euclidean dual of \mathcal{C} .

Proof. For $h(t) = \sum_{i=0}^k h_i t^i$ and $f(t) = \sum_{i=0}^m a_i t^i$ we have

$$\begin{aligned} t^k \theta(h(t)) \theta(g(t)) t^{m-k} &= t^k \theta(g(t) h(t)) t^{m-k} = t^k \theta\left(\sum_{i=0}^m a_i t^i\right) t^{m-k} \\ &= t^k \theta\left(\sum_{i=0}^m t^{-i} a_i\right) t^{m-k} = \sum_{i=0}^m \sigma^{m-k-i}(a_{m-i}) t^i = \sigma^{-k}(a_0) \left(\sum_{i=0}^m \sigma^{-k}(a_0) \sigma^{m-k-i}(a_{m-i}) t^i\right) = a_0^{-1} l(t). \end{aligned}$$

The monic polynomial l on the right-hand side of this equation equals f if and only if for all i , $0 \leq i \leq m$,

$$a_i = a_0^{-1} \sigma^{m-k-i}(a_{m-i}).$$

Let $g^\perp(t) = t^k \theta(h(t)) \in S[t^{-1}; \sigma^{-1}]$, then

$$g^\perp(t) = t^k \sum_{i=0}^k t^{-i} h_i = \sum_{i=0}^k t^{k-i} h_i = \sum_{i=0}^k \sigma^{i-k}(h_i) t^{k-i} = \sum_{j=0}^k \sigma^{-j}(h_{k-j}) t^j.$$

Since $a_0^{-1} \in \text{Fix}(\sigma)$ is invertible, we know that

$$g^\perp(t) \theta(g(t)) t^{m-k} = \sigma^{-k}(a_0) f(t) = f(t) \sigma^{-k}(a_0),$$

so that $g^\perp(t) \theta(g(t)) t^{m-k} a_0^{-1} = f(t)$ shows that $g^\perp(t)$ is a left divisor of f . By assumption, $g^\perp(t)$ is also a right divisor of f and is thus associated to a cyclic $(f, \sigma, 0)$ -code. To prove that this code is the dual of \mathcal{C} , is then verbatim to the proof of [14, Proposition 3]. \square

Remark 18. (i) Conditions (i) and (ii) imply that $a_0^2 = 1$ for any integral domain S , hence $a_0 = \pm 1$ when $a_0 \in \mathcal{O}_F/\mathfrak{p}\mathcal{O}_F$ which is a finite field.

(ii) Note that for $f(t) = t^m - a_0$, $a_0 \in \text{Fix}(\sigma) = \mathcal{O}_F/\mathfrak{p}\mathcal{O}_F$ non-zero, this is [14, Proposition 2].

If we now take the map

$$\rho : \Lambda \longrightarrow \Psi(\Lambda/\mathfrak{p}\Lambda) = (\mathcal{O}_K/\mathfrak{p}\mathcal{O}_K)[t, \bar{\sigma}]/(\mathcal{O}_K/\mathfrak{p}\mathcal{O}_K)[t, \bar{\sigma}]\bar{f}$$

and the \mathbb{Z} -lattice $L = \rho^{-1}(\mathcal{C})$ obtained from \mathcal{C} as above, then also $L' = \rho^{-1}(\mathcal{C}^\perp)$ is a \mathbb{Z} -lattice and analogously as stated in [14, Lemma 4.3], clearly

$$\mathcal{C} \subset \mathcal{C}^\perp \text{ implies } L \subset L'.$$

7. CONCLUSION

We presented a method how to construct a lattice from a suitable (f, σ, δ) -code defined over a finite ring which can be seen as a generalization of the classical construction A. This can be summarized as follows: Let D be a cyclic division algebra over F which is already defined over \mathcal{O}_F , or a Galois field extension and f defined over its ring of integers. Take the additional assumptions on σ and δ as given in the corresponding previous sections.

- Choose some monic skew polynomial $f \in \mathcal{D}[t; \sigma, \delta]$ (resp., $f \in \mathcal{O}_K[t; \sigma, \delta]$ in the field case) which is irreducible in $D[t; \sigma, \delta]$.
- Take a natural order Λ of S_f .
- Choose a prime ideal \mathfrak{p} in S_0 . The choice of will influence which finite ring $\mathcal{O}_K/\mathfrak{p}\mathcal{O}_K$ you consider the code \mathcal{C} to be defined over. \overline{f} must be reducible in $(\mathcal{D}/\mathfrak{p}\mathcal{D})[t; \overline{\sigma}, \overline{\delta}]$.
- Choose a principal left ideal \mathcal{I} of Λ such that $\mathfrak{p} \subset \mathcal{I} \cap S_0$.
- $\Psi(\mathcal{I}/\mathfrak{p}\Lambda)$ corresponds to an $(\overline{f}, \overline{\sigma}, \overline{\delta})$ -code \mathcal{C} over $\mathcal{O}_K/\mathfrak{p}\mathcal{O}_K$, and $L = \rho^{-1}(\mathcal{C}) = \mathcal{I}$ is a \mathbb{Z} -lattice whose embedding into \mathbb{R}^N is canonically determined by $S_f \otimes_{\mathbb{Q}} \mathbb{R}$.

If we want to apply this construction to space time block coding instead, we substitute the last step with:

- Take the matrix representing left multiplication in Λ and let \mathcal{C} be the associated space-time block code. Then $\rho^{-1}(\mathcal{C}) = \mathcal{I}$ is a fully diverse space-time block code which is a \mathbb{Z} -lattice.

If desired, this method can be extended to work for any Noetherian integral domain and central simple algebra D over its quotient field. It can be applied for coset coding and wiretap coding analogously as described in [14, Sections 5.2, 5.3].

It would be interesting to investigate which properties of \mathcal{C} carry over to the lattice L and find examples of well performing coset codes.

REFERENCES

- [1] A. S. Amitsur, *Differential polynomials and division algebras*. Annals of Mathematics, Vol. 59 (2) (1954) 245-278.
- [2] A. S. Amitsur, *Non-commutative cyclic fields*. Duke Math. J. 21 (1954), 87105.
- [3] M. Bhaintwal, *Skew quasi-cyclic codes over Galois rings*. Des. Codes Cryptogr. 62 (1) (2012), 85-101.
- [4] A. Batoul, K. Guenda, T. A. Gulliver, *On self-dual cyclic codes over finite chain rings*. Des. Codes Cryptogr. 70 (3) (2014), 347-358.
- [5] D. Boucher, P. Solè, F. Ulmer, *Skew-constacyclic codes over Galois rings*. Adv. Math. Comm. 2 (3) (2008), 273-292.
- [6] D. Boucher, F. Ulmer, *Linear codes using skew polynomials with automorphisms and derivations*, Des. Codes Cryptogr. 70 (3) (2014), 405-431.
- [7] D. Boucher, F. Ulmer, *Self-dual skew codes and factorization of skew polynomials*, J. Symbolic Comput. 60 (2014), 47-61.
- [8] D. Boucher, F. Ulmer, *Coding with skew polynomial rings*, J. Symbolic Comput. 44 (12) (2009), 1644-1656.
- [9] D. Boucher, F. Ulmer, *Codes as modules over skew polynomial rings*. *Cryptography and coding*, Lecture Notes in Comput. Sci., 5921, Springer, Berlin, 2009, 38-55.
- [10] M. Boulagouaz, A. Leroy, *(σ, δ) -codes*. Adv. Math. Comm. 7 (4) (2013), 463-474.
- [11] Y. Cao, *On constacyclic codes over finite chain rings*. Finite Fields Appl. 24 (2013), 124-135
- [12] J. H. Conway, N. J. Sloane, *Sphere packings, Lattices and groups*. Springer Verlag 1999.

- [13] J. Ducoat, F. Oggier, *Lattice encoding of cyclic codes from skew polynomial rings*. Proc. of the 4th International Castle Meeting on Coding Theory and Applications, Palmela, 2014.
- [14] J. Ducoat, F. Oggier, *On skew polynomial codes and lattices from quotients of cyclic division algebras*. Adv. Math. Comm. 10 (1) 2016, 79-94.
- [15] N. Fogarty, H. Gluesing-Luerssen, *A Circulant Approach to Skew-Constacyclic Codes*. Finite Fields Appl. 35 (2015), 92114.
- [16] J. Gao, Kong, *Qiong 1-generator quasi-cyclic codes over $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m} + \cdots + u^{s-1}\mathbb{F}_{p^m}$* . J. Franklin Inst. 350 (10) (2013), 3260-3276.
- [17] Hoechsmann, Klaus, *Simple algebras and derivations*. Trans. Amer. Math. Soc. 108 (1963), 1-12.
- [18] N. Jacobson, "Finite-dimensional division algebras over fields," Springer Verlag, Berlin-Heidelberg-New York, 1996.
- [19] X. Liu, H. Liu, *LCD codes over finite chain rings*. Finite Fields Appl. 34 (2015), 1-19.
- [20] N. Markin, F. Oggier, *Iterated Space-Time Code Constructions from Cyclic Algebras*. IEEE Transactions on Information Theory, 59 (9), September 2013.
- [21] F. Oggier, B. A. Sethuraman, *Quotients of orders in cyclic algebras and space-time codes*. Adv. Math. Commun. 7 (4) (2013), 441-461.
- [22] F. Oggier, J.-C. Belfiore, *Enabling multiplication in lattice codes via Construction A*. IEEE Int. Workshop Inf. Theory 2013, 1-5.
- [23] O. Ore, *Formale Theorie der linearen Differentialgleichungen. (Zweiter Teil)*. (German) J. Reine Angew. Math. 168 (1932), 233-252.
- [24] J.-C. Petit, *Sur certains quasi-corps généralisant un type d'anneau-quotient*, Séminaire Dubriel. Algèbre et théorie des nombres 20 (1966-67), 1-18.
- [25] J.-C. Petit, *Sur les quasi-corps distributifs à base momogène*, C. R. Acad. Sc. Paris 266 (1968), Série A, 402-404.
- [26] S. Pumplün, A. Steele, *Fast-decodable MIDO codes from nonassociative algebras*. Int. J. of Information and Coding Theory (IJICOT) 3 (1) 2015, 15-38.
- [27] S. Pumplün, A. Steele, *The nonassociative algebras used to build fast-decodable space-time block codes*. Adv. Math. Comm. 9 (4) (2015), 449-469.
- [28] S. Pumplün, *How to obtain division algebras used for fast decodable space-time block codes*. Adv. Math. Comm. 8 (3) (2014), 323 - 342.
- [29] S. Pumplün, *A note on linear codes and nonassociative algebras obtained from skew-polynomial rings*. Online at arXiv:1504.00190[cs.IT]
- [30] S. Pumplün, *Finite nonassociative algebras obtained from skew polynomials and possible applications to (f, σ, δ) -codes*. Online at arXiv:1507.01491[cs.IT]
- [31] R. Sandler, *Autotopism groups of some finite non-associative algebras*. American Journal of Mathematics 84 (1962), 239-264.
- [32] R.D. Schafer, "An Introduction to Nonassociative Algebras," Dover Publ., Inc., New York, 1995.
- [33] K. P. Srinath, B. S. Rajan, *Fast-decodable MIDO codes with large coding gain*. IEEE Transactions on Information Theory (2) 60 2014, 992-1007.
- [34] A. Steele, S. Pumplün, F. Oggier, *MIDO space-time codes from associative and non-associative cyclic algebras*. Information Theory Workshop (ITW) 2012 IEEE (2012), 192-196.
- [35] A. Steele, *Nonassociative cyclic algebras*. Israel J. Math. 200 (1) (2014), 361-387.
- [36] W.C. Waterhouse, *Nonassociative quaternion algebras*. Algebras, Groups and Geometries 4 (1987), 365-378.

- [37] M. Wu, *Free cyclic codes as invariant submodules over finite chain rings*. Int. Math. Forum 8 (37-40) (2013), 1835-1838.

E-mail address: `susanne.pumpluen@nottingham.ac.uk`

SCHOOL OF MATHEMATICAL SCIENCES, UNIVERSITY OF NOTTINGHAM, UNIVERSITY PARK, NOTTINGHAM NG7 2RD, UNITED KINGDOM